

UNITED STATES DISTRICT COURT

for the

Northern District of Oklahoma

In the Matter of the Search of)
Data, Records, and Information Forensically Extracted)
from a Device, Currently Stored on a Hard Drive at)
Homeland Security Investigations Tulsa, 125 West 15th)
Street, Suite 500, Tulsa, Oklahoma)

Case No. 24-mj-134-SH**FILED UNDER SEAL**

FILED
 MAR 01 2023
 Mark C. McCartt, Clerk
 U.S. DISTRICT COURT

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (*identify the person or describe the property to be searched and give its location*):

See Attachment "A"

located in the Northern District of Oklahoma, there is now concealed (*identify the person or describe the property to be seized*):

See Attachment "B"

The basis for the search under Fed. R. Crim. P. 41(c) is (*check one or more*):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

*Code Section**Offense Description*

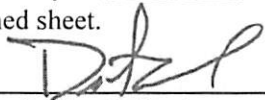
18 U.S.C. § 2422(b)

Coercion and Enticement of a Minor

The application is based on these facts:

See Affidavit of Special Agent Dustin L. Carder, attached hereto.

- ☒ Continued on the attached sheet.
☐ Delayed notice of ____ days (give exact ending date if more than 30 days: ____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

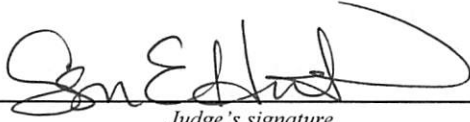

 Applicant's signature

Dustin L. Carder, Special Agent, HSI

Printed name and title

Subscribed and sworn to by phone.

Date: 3/1/24


 Judge's signature

City and state: Tulsa, Oklahoma

Susan E. Huntzman, U.S. Magistrate Judge

Printed name and title

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF OKLAHOMA**

**In the Matter of the Search of
Data, Records, and Information
Forensically Extracted from a Device,
Currently Stored on a Hard Drive at
Homeland Security Investigations –
Tulsa, Oklahoma**

Case No. _____

FILED UNDER SEAL

**Affidavit in Support of an Application
Under Rule 41 for a Warrant to Search and Seize**

I, Dustin L. Carder, being first duly sworn under oath, depose and state:

Introduction and Agent Background

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant authorizing the examination of property—data, records, and information forensically extracted from a device—which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a federal law enforcement officer as defined under Rule 41(a)(2)(C) and am authorized to request this search warrant because I am a government agent who is engaged in enforcing federal criminal laws and I am within the category of officers authorized by the Attorney General to request such a warrant.

3. I have been employed as a Special Agent ("SA") with Homeland Security Investigations ("HSI") since December 2018. I am currently assigned to the Office of the Resident Agent in Charge in Tulsa, Oklahoma, and am currently assigned to investigate crimes involving child exploitation. While employed by HSI, I have

investigated federal criminal violations related to child exploitation and child pornography. I have gained experience through training at the Federal Law Enforcement Training Center's (FLETC) twelve-week Criminal Investigator Training Program (CITP) and the sixteen-week Homeland Security Investigations Special Agent Training (HSISAT) program, and everyday work relating to conducting these types of investigations. I have received training in the area of child pornography and child exploitation and have observed and reviewed numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media. I have received focused child exploitation training covering topics such as: interview techniques, live streaming investigations, undercover investigations, capturing digital evidence, transnational child sex offenders, and mobile messaging platforms utilized by these types of offenders.

4. I am familiar with the facts and circumstances of this investigation. The facts set forth in this affidavit are based on my personal observations, knowledge obtained from other law enforcement officers, my review of documents related to this investigation, conversations with others who have personal knowledge of the events and circumstances described herein, and a review of open-source information including information available on the Internet. Because this affidavit is submitted for the limited purpose of establishing probable cause in support of the application for a search warrant, it does not set forth each and every fact I or others have learned during the course of this investigation.

5. Based on my training, experience, and the facts set forth in this affidavit, there is probable cause to believe that evidence of violations of 18 U.S.C. § 2422(b) (Coercion and Enticement of a Minor) will be located in the electronically stored information described in Attachment B and is recorded on the device described in Attachment A.

Identification of the Device to be Examined

6. The property to be searched is records, data, and information forensically extracted from an Apple iPhone 12 lawfully seized from Brandon PRESLEY on February 23, 2024; the data is stored on a hard drive in the possession of HSI Special Agent Dustin Carder, hereinafter the “data.” The data is currently located at Homeland Security Investigations Tulsa, 125 West 15th Street, Suite 500, Tulsa, Oklahoma.

7. The applied-for warrant would authorize the expanded review of the data for the purpose of identifying electronically stored data particularly described in Attachment B.

Technical Terms

8. The following definitions apply to this Affidavit and Attachment B:

- a. “Chat,” as used herein, refers to any kind of text communication over the Internet that is transmitted in real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

b. “Cloud-based storage service,” as used herein, refers to a publicly accessible, online storage provider that collectors of child pornography can use to store and trade child pornography in larger volumes. Users of such a service can share links and associated passwords to their stored files with other traders of child pornography in order to grant access to their collections. Such services allow individuals to easily access these files through a wide variety of electronic devices such as desktop and laptop computers, mobile phones, and tablets, anywhere and at any time. An individual with the password to a file stored on a cloud-based service does not need to be a user of the service to access the file. Access is free and readily available to anyone who has an Internet connection.

c. “Computer,” as used herein, refers to “an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device” and includes smartphones, and mobile phones and devices. *See* 18 U.S.C. § 1030(e)(1).

d. “Computer hardware,” as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices);

peripheral input/output devices (including keyboards, printers, video display monitors, and related communications devices such as cables and connections); any device that can be used to connect to the Internet including a router and a modem; as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).

e. “Computer passwords and data security devices,” as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates “test” keys or “hot” keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

f. “File Transfer Protocol” (“FTP”), as used herein, is a standard network protocol used to transfer computer files from one host to another over a computer network, such as the Internet. FTP is built on client-server architecture and uses separate control and data connections between the client and the server.

g. “Hashtag,” as used herein, refers to a word or phrase preceded by a hash or pound sign (#), which is used to identify messages or groups on a specific topic.

h. “Internet Protocol address” or “IP address,” as used herein, refers to a unique number used by a computer or other digital device to access the Internet. IP addresses can be “dynamic,” meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be “static,” if an ISP assigns a user’s computer a particular IP address that is used each time the computer accesses the Internet.

i. “Internet Service Providers” (“ISPs”), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment.

j. “Minor,” as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

k. “Mobile applications,” as used herein, are small, specialized programs downloaded onto mobile devices that enable users to perform a variety of functions, including engaging in online chat, reading a book, or playing a game.

l. “Records,” “documents,” and “materials,” as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

m. “Remote Computing Service” (“RCS”), as defined in 18 U.S.C. § 2711(2), is the provision to the public of computer storage or processing services by means of an electronic communications system.

n. “Sexually explicit conduct,” as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person.

o. “Visual depiction,” as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether stored in a permanent format.

**Background on Child Pornography,
Computers, the Internet and Email**

9. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience, and knowledge, I know the following:

a. Computers and digital technology have dramatically changed the way in which individuals interested in children interact with each other. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

b. Child pornographers can now transfer printed photographs into a computer-readable format with a device known as a scanner. Furthermore, with the advent of digital cameras and smartphones with cameras, when the photograph is taken

it is saved as a digital file that can be directly transferred to a computer by simply connecting the camera or smartphone to the computer. In the last ten years, the resolution of pictures taken by digital cameras and smartphones has increased dramatically, meaning that such pictures have become sharper and crisper.

Photos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These memory cards often store in excess of 300 gigabytes of data, which provides enough space to store thousands of high-resolution photographs. Video camcorders, which once recorded video onto tapes or mini-CDs, now can save video footage in a digital format directly to a hard drive in the camera. The video files can be easily transferred from the camcorder to a computer.

c. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child pornography. Child pornography can be transferred via electronic mail or through file transfer protocols (FTPs) to anyone with access to a computer and modem. Because of the proliferation of commercial services that provide electronic mail service, chat services (i.e., “instant messaging”), and easy access to the Internet, the computer is a preferred method of distribution and receipt of child pornographic materials.

d. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution. In addition, there are numerous options available for the storage of computer or digital files. One-terabyte external and internal hard drives are not uncommon. Other media storage devices include CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices which are plugged into a port on the computer. It is extremely easy for an individual to take a photo or a video with a digital camera or camera-bearing smartphone, upload that photo or video to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices (CDs and DVDs are unique in that special software must be used to save or "burn" files onto them). Media storage devices can easily be concealed and carried on an individual's person. Smartphones and/or mobile phones are also often carried on an individual's person.

e. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

f. Individuals also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo! and Hotmail, among others. The online services allow a user to set up an account with a remote

computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer or external media in most cases.

g. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional (i.e., by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files). Digital information can also be retained unintentionally such as the traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

h. A device known as a router in conjunction with a modem allows numerous computers to connect the Internet and other computers through the use of telephone, cable, or wireless connection. A router, in conjunction with a modem, can connect literally millions of computers around the world. Routers often store information as to which computer used a modem to connect to the Internet at a specific time and location. This information when viewed along with the traces or

“footprints” can provide valuable information on who distributed and/or received a visual depiction of a minor engaged in sexually explicit conduct and who possessed and accessed with intent to view a visual depiction of a minor engaged in sexually explicit conduct.

Specifics of Search and Seizure of Computer Systems

10. Based upon my training and experience, and information relayed to me by agents and others involved in the forensic examination of computers, I know that computer data can be stored on a variety of systems and storage devices, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact disks, magnetic tapes, memory cards, memory chips, and online or offsite storage servers maintained by corporations, including but not limited to “cloud” storage. I also know that during the search of the premises it is not always possible to search computer equipment and storage devices for data for a number of reasons, including the following:

- a. Searching computer systems is a highly technical process which requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search site all of the technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with

computer personnel who have specific expertise in the type of computer, software application, or operating system that is being searched;

b. Searching computer systems requires the use of precise, scientific procedures which are designed to maintain the integrity of the evidence and to recover “hidden,” erased, compressed, encrypted, or password-protected data. Computer hardware and storage devices may contain “booby traps” that destroy or alter data if certain procedures are not scrupulously followed. Since computer data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted;

c. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises; and

d. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension “.jpg” often are image files; however, a user can easily change the extension to “.txt” to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a “dongle” or “keycard,” is necessary to decrypt the data into readable form. In addition, computer users can conceal data within

another seemingly unrelated and innocuous file in a process called “steganography.” For example, by using steganography a computer user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is contraband, evidence, fruits, or instrumentalities of a crime.

11. Based on my experience and my consultation with other agents and officers who have been involved in computer searches, searching computerized information for contraband, evidence, fruits, or instrumentalities of a crime often requires the seizure of all of a computer system’s input and output peripheral devices, related software, documentation, and data security devices (including passwords), so that a qualified computer expert can accurately retrieve the system’s data in a laboratory or other controlled environment. There are several reasons that compel this conclusion:

a. The peripheral devices that allow users to enter or retrieve data from the storage devices vary widely in their compatibility with other hardware and software. Many system storage devices require particular input/output devices in order to read the data on the system. It is important that the analyst be able to properly re-configure the system as it now operates in order to accurately retrieve the evidence listed above. In addition, the analyst needs the relevant system software (operating systems, interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether

stored on hard drives or on external media), as well as all related instruction manuals or other documentation and data security devices; and

b. In order to fully retrieve data from a computer system, the analyst also needs all magnetic storage devices, as well as the central processing unit (CPU).

Further, the analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software that may have been used to create the data (whether stored on hard drives or on external media) for proper data retrieval.

12. Additionally, based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers, I know that routers, modems, and network equipment used to connect computers to the Internet often provide valuable evidence of, and are instrumentalities of, a crime. This is equally true of so-called "wireless routers," which create localized networks that allow individuals to connect to the Internet wirelessly. Though wireless networks may be "secured" (in that they require an individual to enter an alphanumeric key or password before gaining access to the network) or "unsecured" (in that an individual may access the wireless network without a key or password), wireless routers for both secured and unsecured wireless networks may yield significant evidence of, or serve as instrumentalities of, a crime—including, for example, serving as the instrument through which the perpetrator of the Internet-based crime connected to the Internet and, potentially, containing logging information regarding the time and date of a perpetrator's network activity as well as

identifying information for the specific device(s) the perpetrator used to access the network. Moreover, I know that individuals who have set up either a secured or unsecured wireless network in their residence are often among the primary users of that wireless network.

Probable Cause

13. On February 15, 2024, I received information from the Bixby Police Department (BPD) in reference to rape that had taken place in Norman, Oklahoma, in Cleveland County (BPD report # 24-0300-OF). I learned that the incident took place at or near the University of Oklahoma campus on February 10, 2024, during a track meet, which the Bixby Public Schools track team participated in along with several other schools.

14. On February 15, 2024, Officer Nathan Jones was notified by his dispatch of an anonymous tipline report. The tip referenced a Bixby Ninth Grade Center student possibly having sex with an adult male on February 10th, 2024.

15. The tip stated that on February 10, 2024, while at a track meet at the University of Oklahoma indoor track, 14-year-old A.A. and a 29-year-old male had sex in his car. The tip reported that both individuals went to his car, and drove to an abandoned parking lot and had sex, then returned to the track meet. The person who made the tip said they knew about the event because A.A. is a friend and told her about it. The tipster also said the male solicited sex from another juvenile female who told him no.

16. The male is someone who often hangs out at Bixby track meets and track practices in his car. The male is not a coach, but sometimes helps out at practices and knows the coaches. The male is said to be a 29-year-old, African American male of average height. The tip included a photograph of the male individual.

17. Based on the tip provided to BPD, the photograph included with the original tip and information provided by A.A., I identified the suspect as Brandon PRESLEY. The photograph submitted with the tip is the same on PRESLEY's current Snapchat public profile under username "bpres26101." I know the 29-year-old man to be Brandon PRESLEY, who I am investigating for sexually exploiting three additional teenage girls. Through that investigation, I know that PRESLEY was a football coach at Bixby Public Schools. PRESLEY was terminated from Bixby Public Schools following his last involvement with a minor child. I also know that PRESLEY is a member by blood of the Muscogee (Creek) Nation, a federally recognized Indian tribe.

18. Based on the tip, Officer Jones contacted L.A., A.A.'s mother, by telephone. He informed her who he was and the reason for calling. L.A. confirmed A.A. was at a track meet in Norman on February 10, 2024. Officer Jones told L.A. there had been an anonymous report that named her daughter, and he told her the nature of the report. L.A. said she did not have any knowledge of that event taking place. L.A. became emotional and was upset by that information.

19. L.A. agreed to come to the BPD to continue speaking instead of talking by telephone. A short time later, L.A. arrived at the BPD. L.A. gave additional details

about the track meet, and stated there were several times A.A. was not with her for an hour or more between events. While speaking with L.A., she stated she would like a medical exam for A.A. based on what may have taken place.

20. While speaking with L.A., she checked Life360¹ and showed Officer Jones a Life360 screenshot from February 10, 2024, which showed A.A. was not in the OU track building between 1034 and 1113 hours on that day.

21. After consulting with detectives, Officer Jones called Domestic Violence Intervention Services (DVIS) and requested to speak with them about a possible sexual assault nurse examination (SANE). The SANE nurse agreed to conduct the examination. L.A. was informed and she agreed to have it done on A.A.

22. After A.A. was with the SANE nurse, L.A. informed Officer Jones of things that A.A. disclosed during the drive to the hospital. L.A. said A.A. has been speaking with a man that she identified as Brandon P for some time. A.A. later identified him as Brandon PRESLEY in a forensic interview. PRESLEY told A.A. that he was 20 years old. A.A. believed that PRESLEY possibly had a sophomore brother that attended Bixby schools.

23. A.A. told L.A. she used a friend's phone to speak with PRESLEY and arrange to meet at the track meet. In a forensic interview, A.A. said that she used a

¹ Life360 Inc. is a San Francisco, California-based American information technology company that provides location-based services, including sharing and notifications, to consumers globally. Its main service is called Life360, a family social networking app released in 2008. It markets itself as the leading family location safety app.

friend's phone to log into A.A.'s Snapchat² account to communicate with PRESLEY. A.A. said that the meeting was arranged a week in advance. A.A. told L.A. during the 1034–1113-hour time frame shown on the Life360 app when she was not in the OU track building, she met PRESLEY they went to an abandoned building nearby and had sex.

24. L.A. stated that during the drive, she asked A.A. if she knew why an officer was speaking with L.A. A.A. replied because something bad happened, and when further asked, A.A. said she did something bad with someone. A.A. explained the bad thing was kissing and having sex, and said she did oral sex as well. A.A. said no protection was used. L.A. asked where they went, and A.A. said it seemed like an abandoned building. L.A. then told A.A. where they were going and why, and that L.A.'s concern was making sure A.A. was safe and healthy. A.A. started crying and L.A. asked what she was thinking, and A.A. said she did not want to be here. When asked what she meant by here, A.A. said "in the world." L.A. asked if A.A. was threatened by PRESLEY, and she said she was not, but he did say something about not telling. A.A. said PRESLEY told her not to tell anyone, because one time a teacher got involved with someone and the teacher got sent away for a long time. Other juveniles were mentioned by A.A. to L.A. during the drive. The other juveniles were not around when it happened.

² Snapchat is an American multimedia instant messaging app and service developed by Snap Inc., originally Snapchat Inc. One of the principal features of Snapchat is that pictures and messages are usually only available for a short time before they become inaccessible to their recipients.

25. The SANE nurse informed Officer Jones that A.A. disclosed she communicated with the male through Snapchat using another phone. A.A. also disclosed to the SANE nurse that the male had pulled out during sex and ejaculated on the rear seat of the vehicle they were in. BPD collected the SANE kit, and it has been submitted to the Oklahoma State Bureau of Investigation (OSBI) forensic laboratory for analysis.

26. A.A.'s phone was provided to BPD and L.A. signed a Consent to Search form for the device. L.A. also provided consent for officers to search A.A.'s Snapchat account. A.A. provided her Snapchat username to Officer Jones. At the time, A.A. could not recall what PRESLEY's username was.

27. On February 16, 2024, A.A. was forensically interviewed at the Child Advocacy Center in Tulsa, Oklahoma. A.A. disclosed that she had been communicating with PRESLEY for a while, and that he knew she was only 14 years old. A.A. believed that PRESLEY was 20 years old because that is what he told her. A.A. stated that his Snapchat username was "bpres" with numbers after it. When PRESLEY arrived at the track meet, he was driving a small blue Chevrolet 4 door sedan, which was the vehicle they had sex in. A.A. believed that they parked at an old pharmacy. They started talking and he asked if she wanted to do anything. When they ended up having sex, both of their pants and underwear were off, and no protection was used. A.A. stated that "stuff" came out of her and went onto the car seat. After it was over, PRESLEY dropped her back off at the track meet.

28. A.A. talked to PRESLEY again the following Monday. PRESLEY told her that he was thinking about Saturday and wanted to meet up with her again, and he talked about having a relationship with her in the future. After learning his true age, A.A. confronted PRESLEY and he said telling her he was 20 was a “miscommunication.”

29. I accessed A.A.’s Snapchat data and located a username of “bpres26101.” This was A.A.’s only Snapchat friend with “bpres” in it. There were no messages observed. However, based on my training and experience, this is not uncommon. Snapchat users routinely delete communication with other parties. If those messages are deleted before the Snapchat account is preserved, the content usually cannot be recovered.

30. L.A. obtained a protective order against PRESLEY in Tulsa County District Court. Tulsa County Sheriff’s Office Deputy Osman received the protective order to serve PRESLEY. His last known address was 212 East 2nd Street, Bixby, Oklahoma, within the Northern District of Oklahoma. Deputy Osman attempted to serve the protective order on February 20, 2024. Deputy Osman contacted a woman at the residence who stated PRESLEY was not there. Deputy Osman left his business card with the woman. A short time later, PRESLEY contacted Deputy Osman from phone number (918) 805-4933. PRESLEY was informed that he had a protective order that he needed to be served.

31. During the previous investigation where PRESLEY is suspected of soliciting at least two additional minor victims for sex utilizing Snapchat, TCSO Detective

Matt Gray was able to determine the phone number associated with PRESLEY's Snapchat account during this time was (918) 805-4933, the same number PRESLEY called Deputy Osman from regarding the protective order. During this investigation, Detective Gray located an address for PRESLEY of 212 East 2nd Street, Bixby, Oklahoma, which is only one block from the Bixby High School. I assisted Detective Gray in this investigation and conducted surveillance at the above address. I observed a small blue Chevrolet 4 door sedan at the location; however, I did not capture the vehicle's tag at that time.

32. With the assistance of an OSBI analyst in searching for Oklahoma vehicle registrations utilizing 212 East 2nd Street, Bixby, Oklahoma, a blue 2018 Chevrolet Sonic bearing Muscogee Creek Nation license plate J1T47, VIN: 1G1JD5SH2J4109605 was located. This vehicle is registered in PRESLEY's father's name, Arthur Presley. Photographs of this vehicle were shown to A.A. and she confirmed this was the vehicle PRESLEY was driving.

33. Although PRESLEY's sexual abuse of A.A. occurred outside of the Northern District of Oklahoma, PRESLEY coerced and enticed A.A. to meet him and engage in sexual acts while in the Northern District of Oklahoma. This is reasonable based on PRESLEY's home location, which lies in the Northern District of Oklahoma. A.A. also attends Bixby Public Schools and resides in the Northern District of Oklahoma.

34. On February 22, 2024, in the Northern District of Oklahoma, I was granted three search and seizure warrants relating to PRESLEY's person and vehicle for

evidence of 18 USC 2422 – Coercion or Enticement of a Minor. The warrants were authorized by the Honorable Susan E. Huntsman, U.S. Magistrate Judge.

35. Search warrant 24-MJ-117-SH authorized the seizure of deoxyribonucleic acid (DNA) from PRESLEY via buccal swab.

36. Search warrant 24-MJ-118-SH authorized the seizure of PRESLEY's vehicle, a blue 2018 Chevrolet Sonic, for photographs of the vehicle and evidence within, swabs or samples of biological evidence such as blood, hair, and body fluids, electronic devices, including cell phones, and the stored communications and files located therein pertaining to PRESLEY and A.A.

37. Search warrant 24-MJ-119-SH authorized the seizure and search of electronic devices, including cell phones, from PRESLEY's person, and the stored communications and files therein pertaining to PRESLEY and A.A.

38. On February 23, 2024, at approximately 1655 hours, Detective Matt Gray, TCSO Deputy Brian Osman, and I came into contact with PRESLEY at the QuikTrip located at 15102 South Memorial Drive, Bixby, Oklahoma. Deputy Osman had a protective order to serve PRESLEY and arranged for PRESLEY to meet him at the location. Detective Gray and I went to the location to serve the above-mentioned search warrants on PRESLEY and his vehicle in furtherance of the investigation.

39. When PRESLEY arrived at the location, he was driving the blue 2018 Chevrolet Sonic that agents possessed a search warrant for; PRESLEY was the sole occupant of the vehicle.

40. As agents approached the vehicle, Detective Gray instructed PRESLEY to step out of the vehicle. PRESLEY complied without incident and was patted down for weapons and searched for any electronic devices. The only electronic item seized from PRESLEY's person was his vehicle key.

41. PRESLEY's cell phone, later determined to be an Apple iPhone 12, was observed in plain view on the front passenger seat, and was plugged into a charging cord. PRESLEY was asked if that was his phone, and he replied, "yes." Deputy Osman then served PRESLEY with the protective order and left the scene.

42. I asked PRESLEY to sit in my vehicle so I could speak with him about what was going on. PRESLEY complied and sat in my vehicle. The encounter was video/audio recorded. I explained that agents had a search warrant for his person and vehicle. I then provided PRESLEY with copies of the warrant for his vehicle and person (the electronic device warrant). I then obtained biographical information from PRESLEY including his full name, date of birth, address, phone number – which he provided as (918) 805-4933, highest level of education (high school), prior arrest history (none), firearms (none), marital status (single), any children (none), employer (Mosquito Militia), coaching status (teaches speed and agility to a few boys), etc.

43. Before any specific questioning occurred, I read PRESLEY his *Miranda Rights* from a provided HSI form and was informed he was not under arrest. PRESLEY wished to have his attorney present for any further questioning, so no additional questioning took place. I then provided PRESLEY with a copy of the search warrant

for his person to obtain his DNA. Detective Gray then obtained two buccal swabs from PRESLEY's mouth while he was seated in my vehicle.

44. PRESLEY inquired how he was going to get home; I stated that he could give him a ride, but he would have to wait until his vehicle was towed from the scene.

PRESLEY agreed and wanted to wait for the vehicle to be towed to get a ride.

Detective Gray, PRESLEY, and I exited my vehicle. PRESLEY sat on the tailgate of my vehicle, while Detective Gray requested a tow truck to respond to the location, and I took initial photographs of the outside and inside of the vehicle.

45. I moved my video/audio recording equipment to the bed of his vehicle to continue to record the encounter outside of the vehicle. While waiting for the tow truck, PRESLEY engaged me in conversation about what was going on. I attempted to explain to PRESLEY that there were two investigations going on, one in the Northern District of Oklahoma, and another in Norman, Oklahoma. PRESLEY was unfamiliar with the SCOTUS *McGirt v. Oklahoma* decision and how that affected him since he is part Native American.

46. During one part of the encounter, I attempted to further explain the protective order to PRESLEY and I went through the document with him. I showed PRESLEY the narrative that is written by the petitioner in order to obtain the emergency protective order. After reading the narrative, PRESLEY commented that what was written was not what happened. I did not ask any questions about it.

47. At another point in the encounter, PRESLEY asked if agents were looking for A.A.'s DNA in his vehicle. I told him yes. PRESLEY stated that he is single now,

but he used to have a girlfriend, so there would be a lot of his DNA in the vehicle.

Upon viewing the backseat of the vehicle, I observed multiple white stains on the back seat.

48. The vehicle was towed from the scene and forensic analysis of the Apple iPhone 12 commenced on February 26, 2024, at HSI Tulsa by HSI Computer Forensic Analyst (CFA) Anthony Meter. CFA Meter provided me with a copy of the extracted data for review.

49. The phone number associated with the device is (918) 805-4933; the Apple ID is brandonpresley5@icloud.com. There are two IMEIs associated with the phone: 353779338642095, and 353779339027718.

50. As it pertains to minor victim A.A., I tagged 1,676 artifacts in the data. These artifacts include A.A.'s Snapchat username as a Snapchat contact, hundreds of 'User Notification Events,' and 'Interactions' where the phone logged each time PRESLEY received a Snapchat notification from A.A., as well as him interacting with the application. The Snaps, or Snapchat messages, were not displayed, only that PRESLEY was sent a Snap. Based on the date/time stamps, it appears that PRESLEY and A.A. began communicating with one another on Snapchat on or about January 24, 2024. The pair exchanged what appears to be hundreds of messages through February 15, 2024.

51. I located an Apple Maps³ logged trip on February 10, 2024, beginning at 3:27 PM with an origin location with coordinates (35.2066318868641, -97.4402455425507). Upon entering these coordinates into Google, the location shows to be the Duck Pond Parking Lot located northwest of the University of Oklahoma's indoor track facility, where A.A. was attending the track meet. The destination location coordinates are (35.2174455242782, -97.4535029822795); upon entering these coordinates into Google, the location shows to be the south side of what appears to be an old CVS Pharmacy, or a Spirit Halloween store located at 700 West Main Street, Norman, Oklahoma. In her forensic interview, A.A. stated that the place where they went appeared to be an old pharmacy. Norman Police Department is attempting to locate any available camera footage in the area that might have captured the incident. According to the Apple Maps record, they arrived at the location at 3:41 PM.

52. There is also a return Apple Maps logged trip on February 10, 2024, beginning at 4:11 PM with an origin location with coordinates (35.2174455242782, -97.4535029822795). Upon entering these coordinates into Google, the location is still the south side of the building at 700 West Main Street, Norman, Oklahoma. The destination coordinates are (35.2066506396715, -97.4403221738894). Upon entering

³ Apple Maps is a web mapping service developed by Apple Inc. The default map system of iOS, iPadOS, macOS, and watchOS, it provides directions and estimated times of arrival for driving, walking, cycling, and public transportation navigation.

these coordinates into Google, the location shows to be the Duck Pond Parking Lot at the University of Oklahoma campus, where he picked A.A. up.

53. After interviewing a minor witness, G.I., on February 27, 2024, I learned that she was also a victim of PRESLEY's. G.I. is a friend of A.A.'s and corroborated A.A.'s account of events, as she was also at the track meet at the University of Oklahoma on February 10, 2024, and A.A. had told her what happened. G.I. stated that she also communicated with PRESLEY on Snapchat and PRESLEY propositioned her more than once for sex. G.I. also sent him a nude image of her buttocks.

54. Upon reviewing the data in PRESLEY's phone, I observed that there are 7,878 Facebook Messenger⁴ messages; 608 GroupMe⁵ messages; 259,799 iOS SMS/MMS⁶ messages; 1,822 Snapchat messages; 401 WhatsApp⁷ messages; 500 Instagram⁸ messages; 387 Twitter (X)⁹ messages; and 53 TikTok¹⁰ messages.

⁴ Messenger, also known as Facebook Messenger, is an American proprietary instant messaging app and platform developed by Meta Platforms. Meta Platforms owns and operates Facebook, a social media application.

⁵ GroupMe is a mobile group messaging app owned by Microsoft. It was launched in May 2010 by the private company GroupMe. With GroupMe, users can send and receive text messages, share photos and videos, and create events or polls within the group.

⁶ iOS is the standard operating system on Apple products. iOS messaging allows for text only messages (SMS), and multimedia, video, and audio messages (MMS).

⁷ WhatsApp is an instant messaging and voice-over-IP service owned by technology conglomerate Meta. It allows users to send text, voice messages and video messages, make voice and video calls, and share images, documents, user locations, and other content.

⁸ Instagram is an photo and video sharing social networking service owned by Meta Platforms. It allows users to upload media that can be edited with filters, be organized by hashtags, and be associated with a location via geographical tagging. Posts can be shared publicly or with preapproved followers.

⁹ Twitter, Inc. was an American social media company based in San Francisco, California. The company operated the social networking service Twitter and previously the Vine short video app and Periscope livestreaming service. Twitter is now known as "X," is an online news and social networking site where people communicate in short messages.

¹⁰ TikTok, whose mainland Chinese counterpart is Douyin, is a short-form video hosting service owned by ByteDance. It hosts user-submitted videos, which can range in duration from 3 seconds to 10 minutes.

55. G.I. mentioned in her interview with me that she, L.Y., and A.A. all communicated with PRESLEY on Snapchat. I knew that P.M. was also mentioned in the Bixby report and that G.I. stated A.A. had also used P.M.'s phone to log into her Snapchat account to talk to PRESLEY. I searched the data for the names of the other possible minor females involved that were listed in the original Bixby Police Department report. For G.I., there were approximately 9,926 artifacts returned; for L.Y., there were approximately 2,637 artifacts returned; and for P.M., there were approximately 17 artifacts returned. There are also 188,710 media files on the device.

56. It is evident that PRESLEY is utilizing Snapchat, an electronic service provider, and his cellular device, an instrument of and utilizing interstate and foreign commerce to coerce and entice minor victims into engaging in sexual activities and/or send him sexually explicit media. Based on my training and experience, most individuals use Snapchat from a cellphone or other portable electronic device. Based on G.I.'s statements, the artifacts found on PRESLEY's phone data involving other minor females, it is reasonable to believe that the remainder of the phone data may contain additional evidence of coercion or enticement of a minor.

57. Due to the restrictions of the original search warrant and the obvious need to search the rest of the data, I am requesting this expanded search warrant to search for any evidence of coercion or enticement of any minor located on the data extracted from PRESLEY's Apple iPhone 12.

Historical Investigations Involving PRESLEY

58. In 2019, PRESLEY was a lay coach for Bixby Public Schools, and was accused of soliciting a minor for sex via Snapchat. Multiple minor victim female students accused PRESLEY of soliciting them and showing up at their residences when their parents were asleep. At least one victim reported performing oral sex on PRESLEY. PRESLEY was banned from Bixby Public Schools property; however, no formal charges were filed against PRESLEY.

59. In July 2022, the Tulsa County Sheriff's Office (TCSO) received a report regarding a 13-year-old minor victim, who reported having sexual communications with an adult male, who received inappropriate photographs of her. The victim stated that the male subject told her he was 16 years old and then said he is actually 18 years old. The victim stated that she met the male two times during the middle of the night when her aunt was asleep. She sat in the male's vehicle with him, and he asked her if she wanted to engage in sexual activity, which she declined. The victim provided the male's Snapchat username. Through legal process and investigation, TCSO Detective Matt Gray was able to identify this suspect as PRESLEY.

60. The data to be searched is currently in the lawful possession of HSI. It came into HSI's possession in the following way: seized during the execution of a search warrant. Therefore, while HSI might already have all necessary authority to examine the Device, I seek this additional warrant out of an abundance of caution to be certain that an examination of the Device will comply with the Fourth Amendment and other applicable laws.

61. The data to be searched is currently stored on a hard drive in my possession at Homeland Security Investigations Tulsa, 125 West 15th Street, Suite 500, Tulsa, Oklahoma, within the Northern District of Oklahoma. In my training and experience, I know that the data to be searched has been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the data first came into the possession of HSI.

Electronic Storage and Forensic Analysis

62. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

63. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how PRESLEY's iPhone was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be in the data to be searched because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

- b. I know that when an individual uses an electronic device to coerce or entice a minor, the individual's electronic device will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The electronic device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The electronic device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that an electronic device used to commit a crime of this type may contain: data that is evidence of how the electronic device was used; data that was sent or received; and other records that indicate the nature of the offense.

64. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the data to be searched consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

65. *Manner of execution.* Because this warrant seeks only permission to examine data already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

66. *Methods of examination.* In conducting this examination, law enforcement personnel may use various methods to locate evidence and instrumentalities of the crime(s) under investigation, including but not limited to undertaking a cursory inspection of all information within the data to be searched. This method is analogous to cursorily inspecting all the files in a file cabinet in an office to determine which paper evidence is subject to seizure. Although law enforcement personnel may use other methods as well, particularly including keyword searches, I know that keyword searches and similar methods are typically inadequate to detect all information subject to seizure. As an initial matter, keyword searches work only for text data, yet many types of files commonly associated with stored cellular device data, such as pictures and videos, do not store as searchable text. Moreover, even as to text data, keyword searches cannot be relied upon to capture all relevant communications associated with a cellular device, as it is impossible to know in advance all of the unique words or phrases investigative subjects will use in their communications. Consequently, often many communications in cellular device data that are relevant to an investigation do not contain any searched keywords.

Conclusion

67. Based on the information above, I submit that there is probable cause for a search warrant authorizing the examination of the data described in Attachment A to seek the items described in Attachment B.

68. I am aware that the recovery of data by a computer forensic analyst takes significant time; much the way recovery of narcotics must later be forensically

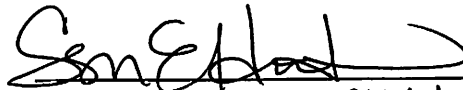
evaluated in a lab, digital evidence will also undergo a similar process. For this reason, the “return” inventory will contain a list of only the tangible items recovered from the premises. Unless otherwise ordered by the Court, the return will not include evidence later examined by a forensic analyst.

Respectfully submitted,



Dustin L. Carder
Special Agent
Homeland Security Investigations

Subscribed and sworn to by phone on March 1, 2024.



SUSAN E. HUNTSMAN
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to be Searched

The property to be searched is records, data, and information forensically extracted from an Apple iPhone 12 lawfully seized from Brandon PRESLEY on February 23, 2024; the data is stored on a hard drive in the possession of HSI Special Agent Dustin Carder, hereinafter the “data.” The data is currently located at Homeland Security Investigations Tulsa, 125 West 15th Street, Suite 500, Tulsa, Oklahoma.

This warrant authorizes the expanded search of the data for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

Particular Things to be Seized

All records in the data described in Attachment A that relate to Title 18 U.S.C. § 2422(b) (enticement of a minor to engage in sexual activity) involving Brandon PRESLEY and any minor, including:

1. Information, correspondence, records, documents, or other materials pertaining to the enticement or coercion of minors to engage in sexual acts or sexual conduct, as defined in 18 U.S.C. 2422(b), that were transmitted or received using the cellular device;
2. Images of child pornography; files containing images and data of any type relating to the sexual exploitation of minors, and material related to the possession or production thereof;
3. Information, correspondence, records, documents, or other materials pertaining to the possession, receipt, or distribution of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C 2256, or pertaining to the sexual exploitation of minors, that were transmitted or received using the cellular device;
4. Evidence of user attribution showing who used or owned the Apple iPhone 12 the data to be search was forensically extracted from at the time the things described in this warrant were created, edited, or deleted, such as logs, phone books, saved usernames and passwords, documents, and browsing history;

5. Records relating to communication with others as to the criminal offense(s) listed above; including incoming and outgoing voice messages; text messages; emails; multimedia messages; applications that serve to allow parties to communicate; all call logs; secondary phone number accounts, and other applications that can assign roaming phone numbers; and other Internet-based communication media;
6. Records relating to documentation or memorialization of the criminal offense(s) listed above, including voice memos, photographs, videos, and other audio and video media, including Exchangeable Image File (“EXIF”) data and any other metadata associated with those photos and videos, including device information, geotagging information, and information about the creation date of the audio and video media;
7. Records relating to the planning and execution of the criminal offense(s) above, including Internet activity, firewall logs, caches, browser history, and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any Internet search engine, records of user-typed web addresses, account information, settings, and saved usage information;
8. Application data relating to the criminal offense(s) above; and
9. All records and information related to the geolocation of the PRESLEY in the data.

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.